Published and Copyright (c) 1999 - 2013
All Rights Reserved

Atari Online News, Etc.
A-ONE Online Magazine
Dana P. Jacobson, Publisher/Managing Editor
Joseph Mirando, Managing Editor
Rob Mahlert, Associate Editor

Atari Online News, Etc. Staff

Dana P. Jacobson -- Editor
Joe Mirando -- "People Are Talking"
Michael Burkley -- "Unabashed Atariophile"
Albert Dayes -- "CC: Classic Chips"
Rob Mahlert -- Web site
Thomas J. Andrews -- "Keeper of the Flame"

With Contributions by:

Fred Horvat

To subscribe to A-ONE, change e-mail addresses, or unsubscribe, log on to our website at: www.atarinews.org and click on "Subscriptions".
OR subscribe to A-ONE by sending a message to: dpj@atarinews.org and your address will be added to the distribution list.
To unsubscribe from A-ONE, send the following: Unsubscribe A-ONE
Please make sure that you include the same address that you used to subscribe from.

To download A-ONE, set your browser bookmarks to one of the following sites:

http://people.delphiforums.com/dpj/a-one.htm
Now available:
http://www.atarinews.org

Visit the Atari Advantage Forum on Delphi!
http://forums.delphiforums.com/atari/

=~=~=~=

A-ONE #1525 06/28/13

~ Working During Vacation ~ People Are Talking! ~ Facebook To Pull Ads!
~ Google Video Game Fight ~ Another Apple-1 Shows! ~ SCO vs. IBM, Part 2!
~ PS3 Not To Be Abandoned ~ WOW Hackers Steal Gold ~ Firefox Hiring Spree!

~ ~ ~

-* Ouya To Shake Up The Industry *-
-* Dark Seoul Gang Hacked South Korea! *-
-* GCHQ Secret Access to World Communications *-

=~=~=~=

->From the Editor’s Keyboard "Saying it like it is!"
""""""""""""""""""""""""""""""

First, another heat wave here in the Northeast, and then thunder, lightning and plenty of rain! And, the weather pattern is showing no immediate plans to improve! Hopefully, things will get somewhat better in time to be able to help celebrate the upcoming 4th of July holiday! I know that, this year especially, the fireworks in Boston are going to be unforgettable! And, I hope to be able to enjoy a terrific barbecue or two!

Until next time...

=~=~=~=

->In This Week’s Gaming Section - Ouya To Shake Up Game Industry?
""""""""""""""""""""""""""""""""" Google Ready for Video Game Fight!
WOW Hackers Steal Millions in Gold!
And more!

=~=~=~=

->A-ONE’s Game Console Industry News - The Latest Gaming News!
""""""""""""""""""""""""""""""""""""""

The $99 Xbox? Ouya’s Affordable Gaming Console Aims to Shake Up an Industry

This holiday season Microsoft launches its $499 Xbox One and Sony its $399 Playstation 4. It’s a big year for gaming fans and, well, a big year for their wallets, especially when you consider that those prices don’t include any of the games.

But starting this week there is a new, significantly more affordable gaming console on the market, which will sit next to those other hotly anticipated systems on Best Buy and Target shelves later this year.

It’s called Ouya (pronounced like Booya, without the B). It costs $99 and it’s nothing like the other consoles in terms of price, performance and offerings. And that’s the point.

"Ouya is a different type of game console. We wanted to bring gaming back to the television by making it accessible to gamers," Julie Uhrman, the founder of Ouya, told ABC News in an interview. "All the games are free to try, and we allow any developer with the creativity and passion to build a game for the television to do so."

Unlike the big clunky Xbox, Wii or Playstation boxes, the Ouya is a small little box, no bigger than other small settop boxes, such as the Apple TV or the Roku. The little vase-shaped device houses the guts of a high-end tablet or smartphone, including an Nvidia quad-core processor and a Wi-Fi radio. There’s no CD or Blu-ray drive - you download the games right to the device.

For $99 you get that box, an HDMI cord to hook it up to your TV and a single, AA-battery-powered controller. Additional controllers will cost $49.95.

The box doesn’t only have some of the same parts as your phone, but it also runs the same software as some of those phones. The menus and all the games have been written on top of Google’s Android platform. But it’s not just a stretched version of the software - the games and the Ouya software have been created for TVs, Uhrman emphasized.

The whole point of using Android, which is an open platform, was to make Ouya an open console. In fact, the O in Ouya stands for "open." The uya? That stands for fun.

The fun, of course, comes with the games. The console launched on Tuesday with more than 160 games, all of which are free to try. "You shouldn’t be gouged by paying $60 for a game if you don’t even know if you like it," Uhrman says, taking a knock at the high-priced console games out there. The only requirement of game makers when submitting games to the Ouya store is that playing some part of it must be free.

But, no, you won’t find "Halo" or "Call of Duty" or "Madden NFL 13" on Ouya. The new console has attracted a range of game makers with experience making games for the PC and game consoles. It also attracts game makers who have never made a game before.

One game available for the console called "Astronaut Rescue" was created by a father and his 8-year-old son. "His son broke his leg skiing, and the dad was like you aren’t going to sit inside all day long and play games, so they decided to build one," Uhrman said.

Joining games like "Astronaut Rescue" are some names that are more familiar to people, such as Sega’s "Sonic the Hedgehog," "Final Fantasy" and "You Don’t Know Jack." The lack of well-known titles might be a sticking point for many, but the free options might be all it takes to bring users in, say some experts.

"The Ouya is attractive because of the $100 price and its free-to-try games. That alone will give people pause enough to consider picking up one of these consoles even though they don’t play the popular games today," Brian Blau, a research director at Gartner, told ABC News.

The first level of Sonic is free, but to unlock all the levels it costs

$6.99. Ouya users are asked to input their credit card numbers during the set-up process.

What you won’t find are a lot of games just brought over from mobile phones, even though the impetus to create the system stemmed from the impact of mobile gaming.

"Games are becoming common on the television. They are sequels, they cost too much to make them - you are getting the same games over and over again," Uhrman says. " We were starting to see more innovative games on mobile platforms because it was easier for developers to create them."

Uhrman, who has spent 10 years in the video game industry, said she began to see game makers leaving their games for consoles and move over to making games for the phone and tablet. She herself found herself playing games on an 8-inch screen with her daughter, rather than on the big TV in front of her. As the industry changed and evolved with people playing on those smaller screens and testing games before buying them, Uhrman believed the entire console market had to be flipped on its head.

Bold words as the brand new Xbox and Playstations make their way to market later this year. However, there are certainly many things the Ouya cannot do that those consoles can. Beyond providing richer games and graphics, they provide more features when it comes to home entertainment, including video and music streaming services. Although Ouya plans to add some of those features soon.

Additionally, early reviews of the Ouya also knock the system for some software and graphics bugs. "There are a few issues that Ouya will need to overcome as quickly as possible. One is this issue of stability," Blau says. "Gamers are a tolerant group but only to an extent."

Still Uhrman believes the console, which is already sold out through Amazon for now, offers something very different for a clear purpose. And, of course, there’s also that other reason to consider it, Uhrman says: "I mean, it’s $99."

Google Is Ready for the Coming Video Game Fight

Apparently with an eye on rumors of Apple entering the video game console business (again), Google is reportedly working on their own Android-based console. Oh, and an Android watch, too, which will also probably have an Apple competitor.

According to the report from the Wall Street Journal (based, of course, on unnamed sources), one of the rumored devices which also includes a Nexus Q media-playing device would be released this fall. But according to the Journal, it looks like the company might have another compelling reason for getting into the game on gaming, at least when it comes to competing with more traditional gaming console makers:

> "Games that run on Android software have proved particularly popular, and they are growing much more quickly than games made for the big-name consoles supplied by Microsoft Corp., Sony Corp. and Nintendo Co. The appeal of such games has prompted the development of new devices aimed specifically for Android by other hardware companies."

Google Play’s store has over 100,000 games already loaded, so the company wouldn’t be hurting for content if they did launch a console. They wouldn’t, however, be the first Android-based console out there. The $99 Ouya, which launched this week, runs a version of Android.

Sony Won t Abandon The PlayStation 3 After The PlayStation 4 Launches

Fear not PlayStation 3 owners, Sony has confirmed that it has no plans to abandon its current console when the PlayStation 4 launches this holiday season for $399. Sony Japan president Hiroshi Kawano and Sony Worldwide president Shuhei Yoshida revealed in an interview with Japanese gaming magazine Weekly Famitsu, translated by Kotaku, that support for the PlayStation 3 will continue indefinitely and the company has no intention of immediately shifting from the PS3 to the PS4. Kawano noted that after seven years the console continues to sell at a constant pace, adding that there are also many upcoming titles are for the system.

With the 2014 launch of our cloud service in the US allowing users to play PS3 games on the PS4, some people may switch consoles from the PS3 to the PS4, Kawano said. But that ll be a gradual process, and to say we re releasing a new console, so trade in your old ones for it would be a maker s ego talking, plain and simple.

Yoshida spoke about the company s decision to require a mandatory PlayStation Plus subscription fee for online play. The executive noted that the service, which had previously been optional, requires a large investment of resources.

Considering the cost, to try to keep such a service free and consequently lower the quality would be absurd, he said. We decided that if that s the case, then it would be better to receive proper payment and continue to offer a good service.

Yoshida was quick to point out, however, that a PlayStation Plus membership would not be required for online play or video services that weren t realtime. He also revealed that if the main account on a system had a PlayStation Plus membership, all other accounts on the PlayStation 4 would receive the same benefits, meaning families won t be required to pay for multiple memberships.

’World of Warcraft’ Hackers Steal Millions in Gold

Adventurers in the online game "World of Warcraft" generally have to worry about bandits and dragons, but their most dangerous threat this week comes in the form of gold-hungry hackers. By exploiting the Web and mobile applications for the game’s Auction House (which allows players to buy and sell items), malefactors have stolen millions of gold pieces, but players who use two-step authentication are relatively safe.

For those who have somehow avoided almost every form of pop culture for the last decade, "World of Warcraft" is a massively popular online game from developer Blizzard that casts players as heroes in an intricate high fantasy world. As players complete quests and triumph over mythical

beasts, they gather in-game gold pieces, which they can use to buy supplies and equipment.

The issue came to light on June 22, when a user named "Abidah" realized that almost 200,000 gold pieces had disappeared from his account for three unauthorized purchases in the game’s Auction House,. He posted his plight on the Blizzard forums, where other users shared similar experiences.

Blizzard investigated, and discovered that while "World of Warcraft" itself had not been compromised, its Web and mobile Auction House apps had. On June 23, Blizzard acknowledged the hack.

"We have taken the Web and Mobile Auction House offline to perform an emergency maintenance," wrote a customer service representative on the forums. "Unfortunately we can’t provide an ETA as to when they will be brought back online."

Blizzard is still not sure how hackers compromised the Auction House apps, but a number of users tell similar stories: After using the Auction House apps, they logged in a few days later to find tons of gold missing from their accounts, often exchanged for absolute junk.

In order to steal gold, the hackers put common, almost worthless items on display at the Auction House. Using players’ compromised accounts, they then bought the item for exponentially more than its in-game worth (a block of wood, for example, is not really worth 50,000 gold pieces).

In all likelihood, the hackers do not want in-game gold for its own sake, but rather want to sell it online in exchange for real money. The only problem with this plan is that Blizzard will usually restore players’ gold if they lost it to a hack. In a large-scale hack, this will essentially duplicate the server’s gold supply, causing massive deflation. Selling gold for real money becomes a profitless endeavor.

The Auction House Web app is now up and running again, but the mobile app remains offline. "At this time we have no reason to believe that accounts currently using an authenticator are at risk," wrote Blizzard in its latest forum update.

An authenticator is a piece of mobile software that users can install to give their Blizzard accounts two-step verification. Each time a user attempts to log into a Blizzard game, he or she must fill out a secondary code that gets sent to a mobile device.

Even this measure may not protect the Auction House hack victims, though. Abidah was quick to point out that he did use an authenticator, and still lost hundreds of thousands of gold pieces. However, his settings required secondary authentication only once a week instead of for every login.

The mobile Auction House should be back up within a few days, users lost no real money and Blizzard will probably restore players’ lost gold. As hacks go, this was on the fairly harmless end of the spectrum, but if hackers have figured out a way around two-step verification, "World of Warcraft" may be in for bigger problems in the future.

=~=~=~=

A-ONE's Headline News
The Latest in Computer Technology News
Compiled by: Dana P. Jacobson

GCHQ Taps Fibre-optic Cables for Secret Access to World's Communications

Britain's spy agency GCHQ has secretly gained access to the network of cables which carry the world's phone calls and internet traffic and has started to process vast streams of sensitive personal information which it is sharing with its American partner, the National Security Agency (NSA).

The sheer scale of the agency's ambition is reflected in the titles of its two principal components: Mastering the Internet and Global Telecoms Exploitation, aimed at scooping up as much online and telephone traffic as possible. This is all being carried out without any form of public acknowledgement or debate.

One key innovation has been GCHQ's ability to tap into and store huge volumes of data drawn from fibre-optic cables for up to 30 days so that it can be sifted and analysed. That operation, codenamed Tempora, has been running for some 18 months.

GCHQ and the NSA are consequently able to access and process vast quantities of communications between entirely innocent people, as well as targeted suspects.

This includes recordings of phone calls, the content of email messages, entries on Facebook and the history of any internet user's access to websites all of which is deemed legal, even though the warrant system was supposed to limit interception to a specified range of targets.

The existence of the programme has been disclosed in documents shown to the Guardian by the NSA whistleblower Edward Snowden as part of his attempt to expose what he has called "the largest programme of suspicionless surveillance in human history".

"It's not just a US problem. The UK has a huge dog in this fight," Snowden told the Guardian. "They [GCHQ] are worse than the US."

However, on Friday a source with knowledge of intelligence argued that the data was collected legally under a system of safeguards, and had provided material that had led to significant breakthroughs in detecting and preventing serious crime.

Britain's technical capacity to tap into the cables that carry the world's communications referred to in the documents as special source exploitation has made GCHQ an intelligence superpower.

By 2010, two years after the project was first trialled, it was able to boast it had the "biggest internet access" of any member of the Five Eyes electronic eavesdropping alliance, comprising the US, UK, Canada, Australia and New Zealand.

UK officials could also claim GCHQ "produces larger amounts of metadata

than NSA". (Metadata describes basic information on who has been contacting whom, without detailing the content.)

By May last year 300 analysts from GCHQ, and 250 from the NSA, had been assigned to sift through the flood of data.

The Americans were given guidelines for its use, but were told in legal briefings by GCHQ lawyers: "We have a light oversight regime compared with the US".

When it came to judging the necessity and proportionality of what they were allowed to look for, would-be American users were told it was "your call".

The Guardian understands that a total of 850,000 NSA employees and US private contractors with top secret clearance had access to GCHQ databases.

The documents reveal that by last year GCHQ was handling 600m "telephone events" each day, had tapped more than 200 fibre-optic cables and was able to process data from at least 46 of them at a time.

Each of the cables carries data at a rate of 10 gigabits per second, so the tapped cables had the capacity, in theory, to deliver more than 21 petabytes a day equivalent to sending all the information in all the books in the British Library 192 times every 24 hours.

And the scale of the programme is constantly increasing as more cables are tapped and GCHQ data storage facilities in the UK and abroad are expanded with the aim of processing terabits (thousands of gigabits) of data at a time.

For the 2 billion users of the world wide web, Tempora represents a window on to their everyday lives, sucking up every form of communication from the fibre-optic cables that ring the world.

The NSA has meanwhile opened a second window, in the form of the Prism operation, revealed earlier this month by the Guardian, from which it secured access to the internal systems of global companies that service the internet.

The GCHQ mass tapping operation has been built up over five years by attaching intercept probes to transatlantic fibre-optic cables where they land on British shores carrying data to western Europe from telephone exchanges and internet servers in north America.

This was done under secret agreements with commercial companies, described in one document as "intercept partners".

The papers seen by the Guardian suggest some companies have been paid for the cost of their co-operation and GCHQ went to great lengths to keep their names secret. They were assigned "sensitive relationship teams" and staff were urged in one internal guidance paper to disguise the origin of "special source" material in their reports for fear that the role of the companies as intercept partners would cause "high-level political fallout".

The source with knowledge of intelligence said on Friday the companies were obliged to co-operate in this operation. They are forbidden from revealing the existence of warrants compelling them to allow GCHQ access

to the cables.

"There’s an overarching condition of the licensing of the companies that they have to co-operate in this. Should they decline, we can compel them to do so. They have no choice."

The source said that although GCHQ was collecting a "vast haystack of data" what they were looking for was "needles".

"Essentially, we have a process that allows us to select a small number of needles in a haystack. We are not looking at every piece of straw. There are certain triggers that allow you to discard or not examine a lot of data so you are just looking at needles. If you had the impression we are reading millions of emails, we are not. There is no intention in this whole programme to use it for looking at UK domestic traffic British people talking to each other," the source said.

He explained that when such "needles" were found a log was made and the interception commissioner could see that log.

"The criteria are security, terror, organised crime. And economic well-being. There’s an auditing process to go back through the logs and see if it was justified or not. The vast majority of the data is discarded without being looked at we simply don’t have the resources."

However, the legitimacy of the operation is in doubt. According to GCHQ’s legal advice, it was given the go-ahead by applying old law to new technology. The 2000 Regulation of Investigatory Powers Act (Ripa) requires the tapping of defined targets to be authorised by a warrant signed by the home secretary or foreign secretary.

However, an obscure clause allows the foreign secretary to sign a certificate for the interception of broad categories of material, as long as one end of the monitored communications is abroad. But the nature of modern fibre-optic communications means that a proportion of internal UK traffic is relayed abroad and then returns through the cables.

Parliament passed the Ripa law to allow GCHQ to trawl for information, but it did so 13 years ago with no inkling of the scale on which GCHQ would attempt to exploit the certificates, enabling it to gather and process data regardless of whether it belongs to identified targets.

The categories of material have included fraud, drug trafficking and terrorism, but the criteria at any one time are secret and are not subject to any public debate. GCHQ’s compliance with the certificates is audited by the agency itself, but the results of those audits are also secret.

An indication of how broad the dragnet can be was laid bare in advice from GCHQ’s lawyers, who said it would be impossible to list the total number of people targeted because "this would be an infinite list which we couldn’t manage".

There is an investigatory powers tribunal to look into complaints that the data gathered by GCHQ has been improperly used, but the agency reassured NSA analysts in the early days of the programme, in 2009: "So far they have always found in our favour".

Historically, the spy agencies have intercepted international communications by focusing on microwave towers and satellites. The NSA’s intercept station at Menwith Hill in North Yorkshire played a leading

role in this. One internal document quotes the head of the NSA, Lieutenant General Keith Alexander, on a visit to Menwith Hill in June 2008, asking: "Why can't we collect all the signals all the time? Sounds like a good summer project for Menwith."

By then, however, satellite interception accounted for only a small part of the network traffic. Most of it now travels on fibre-optic cables, and the UK's position on the western edge of Europe gave it natural access to cables emerging from the Atlantic.

The data collected provides a powerful tool in the hands of the security agencies, enabling them to sift for evidence of serious crime. According to the source, it has allowed them to discover new techniques used by terrorists to avoid security checks and to identify terrorists planning atrocities. It has also been used against child exploitation networks and in the field of cyberdefence.

It was claimed on Friday that it directly led to the arrest and imprisonment of a cell in the Midlands who were planning co-ordinated attacks; to the arrest of five Luton-based individuals preparing acts of terror, and to the arrest of three London-based people planning attacks prior to the Olympics.

As the probes began to generate data, GCHQ set up a three-year trial at the GCHQ station in Bude, Cornwall. By the summer of 2011, GCHQ had probes attached to more than 200 internet links, each carrying data at 10 gigabits a second. "This is a massive amount of data!" as one internal slideshow put it. That summer, it brought NSA analysts into the Bude trials. In the autumn of 2011, it launched Tempora as a mainstream programme, shared with the Americans.

The intercept probes on the transatlantic cables gave GCHQ access to its special source exploitation. Tempora allowed the agency to set up internet buffers so it could not simply watch the data live but also store it for three days in the case of content and 30 days for metadata.

"Internet buffers represent an exciting opportunity to get direct access to enormous amounts of GCHQ's special source data," one document explained.

The processing centres apply a series of sophisticated computer programmes in order to filter the material through what is known as MVR massive volume reduction. The first filter immediately rejects high-volume, low-value traffic, such as peer-to-peer downloads, which reduces the volume by about 30%. Others pull out packets of information relating to "selectors" search terms including subjects, phone numbers and email addresses of interest. Some 40,000 of these were chosen by GCHQ and 31,000 by the NSA. Most of the information extracted is "content", such as recordings of phone calls or the substance of email messages. The rest is metadata.

The GCHQ documents that the Guardian has seen illustrate a constant effort to build up storage capacity at the stations at Cheltenham, Bude and at one overseas location, as well a search for ways to maintain the agency's comparative advantage as the world's leading communications companies increasingly route their cables through Asia to cut costs. Meanwhile, technical work is ongoing to expand GCHQ's capacity to ingest data from new super cables carrying data at 100 gigabits a second. As one training slide told new users: "You are in an enviable position have fun and make the most of it."

Facebook To Pull Ads from Pages with Sex, Violence

Facebook Inc said it will no longer allow ads to appear on pages with sexual or violent content, as the online social network moves to appease marketers being associated with objectionable material.

The moves come a month after several businesses pulled their ads from Facebook amid reports of pages on Facebook that promoted violence against women.

Facebook said at the time that it needed to improve its system for flagging and removing content that violated its community standards, which forbid users from posting content about hate-speech, threats and pornography, among other things.

Ads account for roughly 85 percent of revenue at Facebook, the world's largest social network with 1.1 billion users. Facebook said the changes would not have a meaningful impact on its business.

On Friday, Facebook said it also needed to do more to prevent situations in which ads are displayed alongside material that may not run afoul of its community standards but are deemed controversial nonetheless.

A Facebook page for a business that sells adult products, for example, will no longer feature ads. Previously such a page could feature ads along the right-hand side of the page so long as the page did not violate Facebook's prohibition on depicting nudity.

The move underscores the delicate balance for social media companies, which features a variety of unpredictable and sometimes unsavory content shared by users, but which rely on advertising to underpin their business.

"Our goal is to both preserve the freedoms of sharing on Facebook but also protect people and brands from certain types of content," Facebook said in a post on its website on Friday.

Facebook said on Friday that it would expand the scope of pages and groups on its website that should be ad-restricted and promised to remove ads from the flagged areas of the website by the end of the coming week.

Pages and groups that reference violence will also be off limits to ads, the company said. A Facebook spokeswoman noted that the policy would not apply to the pages of news organizations on Facebook.

Facebook said the process of flagging objectionable pages and removing ads would initially be done manually, but that the company will build an automated system to do the job in the coming weeks.

Four-year Hacking Spree in South Korea Blamed on 'Dark Seoul Gang'

Researchers with U.S. security software maker Symantec Corp say they have uncovered digital evidence that links cyber attacks on South Korea dating

back four years to a single hacking group dubbed the "Dark Seoul Gang."

Eric Chien, technical director with Symantec Security Response, said late on Wednesday that his firm made the connection while reviewing malicious software code used to launch attacks that disrupted some South Korean government websites earlier in the week.

He said that the evidence did not uncover the identity of the gang members.

North Korea has been blamed for previous cyber attacks on South Korean banks and government networks, although Pyongyang denies responsibility and has said it has also been a victim.

Symantec researchers found chunks of code that were identical to code in malicious programs used in four previous significant attacks, the first of which happened on July 4, 2009, according to Chien.

"We know that they are one gang," he said. "It is extremely well coordinated."

He estimates that the group has between 10 and 50 members, based on the sophistication of the code and the complexity of their attacks.

The July 4, 2009, attack wiped data on PCs and also launched distributed denial of service attacks that disrupted websites in South Korea as well as the United States.

In March of this year, the gang knocked tens of thousands of PCs off line at South Korean companies by destroying data on their hard drives, Chien said. It was one of the most destructive cyber attacks on private computer networks to date.

Symantec published its report on the gang on its website: http://bit.ly/14ukq4o

A hacking attack on Tuesday, the anniversary of the start of the Korean War in 1950, brought down the main websites of South Korea’s presidential office and some local newspapers, prompting cybersecurity officials to raise the alert.

Worst Sequel Ever: SCO vs. IBM Reopened

For the last several months, we have consistently stated and maintained that our System V code is in Linux. The claims SCO has are both broad and deep. These claims touch not just IBM but other vendors as well. They also touch certain industry consortia and corporate Linux end users. Our claims aren t trivial. The violations of our intellectual property are not easily repaired. It is our intention to vigorously protect and enforce SCO s intellectual property, System V source code and our copyrights. We re now fully prepared to do that.

Former SCO CEO Darl McBride, in 2003

When the SCO Group which for a decade waged an aggressive and ill-starred legal campaign against the Linux OS collapsed into financial ruin last summer, it seemed that the company was finally headed for an

ignominious grave. Following hard-fought but ultimately ludicrous lawsuits against both Novell and IBM, SCO careened from Chapter 11 into Chapter 7 bankruptcy, volunteering in its own filing that it had no reasonable chance of rehabilitation.

But evidently liquidation wasn t enough to keep SCO dead and buried, because this past May the company filed a request to reopen its case against IBM. Now a Utah district court judge has granted it, and SCO is clambering from the grave and preparing to shamble into court after IBM once again.

Astonishing. You d think that after all these years, SCO would be little more than a case study in why using litigation as a profit center to compensate for market losses is bad business. But no. It s back. And once again, it s pushing forward with its suit accusing IBM of misappropriation of trade secrets, unfair competition, breach of contract and tortious interference. And the end game here is the same as it has always been: Squeeze millions of dollars in licensing fees from a company it claims illegally distributed portions of its proprietary Unix code with the Linux OS code it has never really specified, despite repeated calls to do so from its defendants and the open source community.

So SCO has been given one last shot at IBM, a chief architect of its ruin. And while it s impossible to say what will become of it, the company s litigation record doesn t bode well for its chances.

As Groklaw editor Pamela Jones quips in her write-up of this latest development in the case, What SCO should really ask the court for is a Time Machine, so it can go back in time and do a better job.

Foxconn s Firefox OS Hiring Spree

Now that electronics manufacturer Foxconn has partnered with Mozilla to develop devices running its Firefox operating system, the company is hiring up in support of that effort.

Foxconn hopes to recruit up to 3,000 software engineers with chops in HTML 5 and cloud computing application programming in the months ahead.

That s triple the headcount the company said it planned to hire when it first announced its partnership with Mozilla. And it speaks to the breadth of its commitment to Firefox OS. Foxconn currently plans to build five Firefox OS devices in support of its eight screens, one network, and one cloud plan. And staffing up its software center in Greater Kaohsiung, Taiwan, is essential to that effort.

 [Foxconn] will do its best to develop the Kaohsiung software center as the company s software powerhouse, the company said in a statement. There will be no budget limit for fostering software talent.

A grand pronouncement for Foxconn, which is best known as a large-scale manufacturing partner to device makers like Apple. And one that suggests that the company is serious about diversifying its business, and not simply to the manufacture of Firefox devices, but seemingly cloud computing services, as well.

How Worker Vacations Put Employers at Risk

Bosses may want to be careful what they wish for when it comes to expecting employees to work through their vacations. New research has found that workers are risking their companies' security when they work while on vacation.

Overall, 77 percent of respondents say they do not have an office network when they are on vacation. However, that is not stopping many workers from accessing work files out of the office. To do this, 32 percent of workers say they access work files via insecure cloud-sharing services like Dropbox, Google Drive or Skydrive. Workers are also putting sensitive work information and files at risk by bringing work computers or business files away on vacation. Just 23 percent of workers say they access files through their corporate network.

Those lax security procedures have the potential to hurt companies in a big way, especially since 59 percent of workers admit to working during vacation. Common work tasks during vacation include checking email and answering phone calls.

Technology is both the reason why workers have been able to more easily work while on vacation and the reason for the security concerns about it. Smartphones and personal laptops are the two most popular devices workers use while on vacation. Tablets and work computers are also helping workers to work on vacation.

"The information age has enabled unprecedented levels of employee productivity from the corner office to the factory floor, but it has also created a dependency on the applications, files and data that employees depend on everyday to get their job done," said Todd Krautkremer, vice president of marketing at Pertino, a provider of cloud services to small and medium-size business that conducted the research. "This can actually lead to anxiety when an employee is disconnected for a protracted period of time."

Workers aren t fully against having access to technology and devices while on vacation, though. Nearly half of respondents say they are less stressed on vacation since they know that they are never too far away from their office and personal devices.

The research was based on more than 1,000 responses.

Another Working Apple-1 Pops Up, Could Sell for $500K

Christie s said it hopes to sell a working Apple-1 computer for as much as half a million dollars in a special online-only auction that starts next week.

The computer, one of fewer than 50 known to have survived from a limited run of about 200, is even rarer in that it works, according to Christie s, which Friday confirmed an account by the Associated Press that the Apple-1 is functional.

Christie s estimated that the rare computer will sell for between $300,000

and $500,000.

That s not impossible: Last month, a working Apple-1 sold at a German auction for $542,000. The total, including a 22.3% commission as well as taxes, paid by the buyer was a record $671,400.

The May sale eclipsed the previous record of $640,000 for an Apple-1 established last November, also at an auction conducted by Auction Team Breker of Cologne, Germany.

Whether the Christie s Apple-1 sets a record or comes close to earlier prices depends on whether the auction attracts the clientele that s been willing to pay premium prices, said Mike Willegal, an Apple-1 expert whose index of existing machines is the world s most complete.

 The question is how many people have that deep of pockets, Willegal said in an email Friday. The last couple of high-dollar Apple-1s went to Korea, so if the publicity gets to Asia, who knows?

Willegal, who keeps tabs on the whereabouts of known Apple-1s, said that the Christie s unit was news to him. This is likely a new one that has surfaced, which is especially likely if it really has been in this man s hands for so long, said Willegal, referring to the AP story. It said the current owner, identified as Ted Perry, had acquired the Apple-1 in 1979 or 1980, and kept it in a cardboard box since then.

Christie s declined to make Perry available for an interview Friday.

But Willegal wasn t surprised that the Apple-1 appeared out of nowhere. I m sure the high selling prices are going to have some additional units popping out of the woodwork, he said.

Apple-1 prices have climbed dramatically since the death of Apple co-founder and former CEO Steve Jobs in 2011. A working Apple-1 sold in November 2010 by Christie s went for $213,000; less than two years later, in June 2012, rival Sotheby s sold a different operational Apple-1 for a then-record $374,500.

That kind of money may eventually prompt fraudsters to shill a forgery or an accurate reproduction as the real thing. I think a reproduction or forgery could be made pretty compelling, but an expert should be able to tell the difference when looking at one in person, said Willegal, who has been approached in the past to authenticate other Apple-1 computers, but has declined because he was asked to do so based only on photographs.

Unlike later personal computers, including the 1977 Apple II, the Apple-1 was sold as a fully-assembled circuit board, but minus a case, power supply, keyboard or monitor. Buyers had to provide those components, resulting in some interesting customizations. Christie s Apple-1 is mounted on a wooden board, as are a modern keyboard and the power supply.

All Apple-1s were hand-built by Apple co-founder Steve Wozniak in 1976. They sold then for $666.66, equivalent to $2,724 in today s dollars, or more than a top-of-the-line 15-inch MacBook Pro with a Retina-quality display goes for now.

The one to be sold by Christie s is hand-signed by Wozniak, as are the included manual and board schematics.

Christie s Apple-1 will be exhibited at the Computer History Museum in

Mountain View, Calif., June 24-27. The online auction runs from June 24 to July 9.

Christie s will put this Apple-1 on the block in an online auction that begins June 24, and has pegged the likely sales price between $300,000 and $500,000.

=~=~=~=

Atari Online News, Etc. is a weekly publication covering the entire Atari community. Reprint permission is granted, unless otherwise noted at the beginning of any article, to Atari user groups and not for profit publications only under the following terms: articles must remain unedited and include the issue number and author at the top of each article reprinted. Other reprints granted upon approval of request. Send requests to: dpj@atarinews.org

No issue of Atari Online News, Etc. may be included on any commercial media, nor uploaded or transmitted to any commercial online service or internet site, in whole or in part, by any agent or means, without the expressed consent or permission from the Publisher or Editor of Atari Online News, Etc.

Opinions presented herein are those of the individual authors and do not necessarily reflect those of the staff, or of the publishers. All material herein is believed to be accurate at the time of publishing.